What is claimed is:

1. A method of detecting critical file changes, comprising:

reading events representing various types of system calls;

routing the event to an appropriate template, the event having multiple parameters;

filtering the event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event; and

creating an intrusion alert if an event is output from said filtering step.

2. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that the permission bits on a file or directory were changed.

3. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that a file was opened for truncation.

4. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that ownership or group ownership of a file has been changed.

5. The method of claim 1, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to.

6. The method of claim 1, comprising configuring templates based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

7. A method of detecting critical file changes, comprising:

reading events including encoded information representing system calls;

routing the event to an appropriate template based on the encoded information;

filtering the event as either a possible intrusion based on the encoded information and either dropping the event or outputting the event; and

creating an intrusion alert of an event is output from said filtering step.

8. The method of claim 7, wherein said filtering step outputs an event if the encoded information indicates that the permission bits on a file or directory were changed.

9. The method of claim 7, wherein said filtering step outputs an event if the encoded information indicates that a file was opened for truncation.

10. The method of claim 7, wherein said filtering step outputs an event of the encoded information indicates that ownership or group ownership of a file has been changed.

11. The method of claim 7, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to.

12. The method of claim 7, comprising configuring templates based a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.